

МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ

Директор института прикладной
математики и компьютерных наук

А.В. Замятин

« 02 » июля 2021 г.

Защита информации от утечки по техническим каналам

рабочая программа дисциплины

Закреплена за кафедрой	<i>компьютерной безопасности</i>
Учебный план	<i>10.05.01 Компьютерная безопасность, профиль «Анализ безопасности компьютерных систем»</i>
Форма обучения	<i>очная</i>
Общая трудоёмкость	<i>3 з.е.</i>
Часов по учебному плану	<i>108</i>
в том числе:	
аудиторная контактная работа	<i>48</i>
самостоятельная работа	<i>57.35</i>
Вид(ы) контроля в семестрах	
<i>экзамен/зачет/зачет с оценкой</i>	<i>Семестр 9 – зачет</i>

Программу составил:
канд. техн. наук,
доцент кафедры компьютерной безопасности



В.А. Беляев

Рецензент:
д-р техн. наук, профессор,
профессор кафедры прикладной математики



В.И. Смагин

Рабочая программа дисциплины «Защита информации от утечки по техническим каналам» разработана в соответствии с образовательным стандартом высшего образования – специалитет, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по специальности 10.05.01 Компьютерная безопасность (Утвержден Ученым советом НИ ТГУ, протокол от 30.06.2021 г. № 06).

Рабочая программа одобрена на заседании кафедры компьютерной безопасности

Протокол от 02 июня 2021 г. № 06

Заведующий кафедрой компьютерной безопасности,
канд. техн. наук, доцент



С.А. Останин

Рабочая программа одобрена на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор



С.П. Сущенко

Цель освоения дисциплины

Цель – освоить основные понятия в области физических явлений и процессов при решении профессиональных задач, познакомиться с основными техническими средствами защиты и особенностями их работы.

– Научиться применению знаний, навыков и умений, необходимых для решения задач инженерно-технической защиты информации с учётом требований системного подхода.

1. Место дисциплины в структуре ОПОП

Дисциплина «Защита информации от утечки по техническим каналам» относится к обязательной части Блока 1 «Дисциплины», входит в модуль «Специализация».

Пререквизиты дисциплины: для успешного усвоения дисциплины обучающиеся должны обладать компетенциями, сформированными при изучении следующих дисциплин и модулей: «Физика», «Основы построения защищённых компьютерных сетей», «Компьютерные сети».

2. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Таблица 1.

Компетенция	Индикатор компетенции	Код и наименование результатов обучения (планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций)
ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ИОПК-4.1 Понимает основные физические законы и модели, выявляет естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности; ИОПК-4.2 Применяет соответствующий физико-математический аппарат для формализации, анализа и выработки решения проблем, возникающих в ходе профессиональной деятельности; ИОПК-4.3 Анализирует физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники.	ОР-1.4.1 Способность понимать основные физические законы и модели, выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности; ОР-1.4.2. Способность применять физико-математический аппарат для формализации, анализа и выработки решения проблем, возникающих в ходе профессиональной деятельности; ОР-1.4.3. Способность анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники.
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.	ИОПК-9.3 Обладает знанием и демонстрирует навыки применения методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	Обладает знанием и демонстрирует навыки применения методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
	9 семестр	всего
Общая трудоемкость	108	108
Контактная работа:	50,65	50,65
Лекции (Л):	32	32
Практики (ПЗ)		
Лабораторные работы (ЛР)	16	16
Семинары (СЗ)		
Групповые консультации		
Индивидуальные консультации	2,65	2,65
Промежуточная аттестация		
Самостоятельная работа обучающегося:	57,35	57,35
Вид промежуточной аттестации (зачет)	Зачет	Зачет

3.2. Содержание и трудоемкость разделов дисциплины

Таблица 3.

Код занятия	Наименование разделов и тем и их содержание	Вид учебной работы, занятий, контроля	С е м е с т р	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
	Раздел 1. Системный подход к защите информации	Лекции	9		2	1	ОР-1.4.1
1.1.	Системный подход к защите информации		9		2		
1.2.	Основные концептуальные положения		9				
	Раздел 2. Технические каналы утечки информации	Лекции	9		3	1,2	ОР-1.4.1, ОР-1.4.2,
2.1.	Информация как предмет защиты		9		2		
2.2.	Источники опасных сигналов		9		1		
2.3.	Технические каналы утечки информации		9				
2.4.	Распространение сигналов в технических каналах утечки информации		9				
2.5.	Средства технической разведки		9				
	Раздел 3. Технические средства защиты информации	Лекции	9		22	1, 2, 3	ОР-1.4.3, ОР-1.4.4, ОР-2.4.1, ОР-2.4.2,
3.1.	Подавление опасных сигналов				5		
3.2.	Аппаратные средства защиты и взлома				1		
3.3.	Средства радиомониторинга				1		
3.4.	Средства инженерной защиты и технической охраны объектов				1		
3.5.	Средства предотвращения утечки информации по техническим каналам				1		
3.6.	Обнаружители пустот, металлодетекторы				2		
3.7.	Оптические каналы утечки информации				2		
3.8.	Принципы оценки эффективности средств защиты информации от утечки по техническим каналам				4		
	Подготовка к промежуточной аттестации в форме зачета	СРС	9		33,7	1, 2, 3	
	Прохождение промежуточной аттестации в форме зачета	З	9		2,3		

4. Образовательные технологии, учебно-методическое и информационное обеспечение для освоения дисциплины

Чтение лекций с использованием презентаций и учебных фильмов. После прослушивания курса лекций выполняется самостоятельная работа студента. Самостоятельная работа включает подготовку реферата по предложенной теме и подготовку доклада по теме реферата в виде файла в формате *.ppt. Работа над рефератом состоит из следующих этапов: подбор литературы (источников), изучение проблем по теме реферата, обобщение собранного материала, составление плана реферата, написание реферата в соответствии с планом. Реферат завершается выводами, в которых необходимо показать отношение **автора реферата** к рассматриваемой проблеме и пути её решения.

Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций, и методические материалы, определяющие процедуры оценивания результатов обучения, приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

4.1. Рекомендуемая литература и учебно-методическое обеспечение

№ п/п	Авторы / составители	Заглавие	Издательство	Год издания, количество страниц
Основная литература				
1.	Каторин Ю.Ф., Разумовский А.В., Спивак А.И.	Защита информации техническими средствами: Учебное пособие	СПб: НИУ ИТМО	2012. – 416 с.
2.	Зайцев А.П.	Технические средства и методы защиты информации	М: Горячая линия-Телеком	2012 г., 615 с.
Дополнительная литература				
3.	Царегородцев А.В.	Технические средства защиты информации. Учебник	М.: Изд. ВГНА Минфина России	2009 – 312 с.

4.2. Базы данных и информационно-справочные системы, в том числе зарубежные

1. Электронная библиотека (репозиторий) ТГУ [Электронный ресурс] / Электронная библиотека (репозиторий) ТГУ : [сайт]. – [Томск, 2011–2016]. – URL: <http://vital.lib.tsu.ru/vital/access/manager/Index>.

4.3. Перечень лицензионного и программного обеспечения

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);

– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

4.4. Оборудование и технические средства обучения

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

5. Методические указания обучающимся по освоению дисциплины

После прослушивания курса лекций выполняется самостоятельная работа студента. Самостоятельная работа включает подготовку реферата по предложенной теме и подготовку доклада по теме реферата в виде файла в формате *.ppt. Работа над рефератом состоит из следующих этапов: подбор литературы (источников), изучение проблем по теме реферата, обобщение собранного материала, составление плана реферата, написание реферата в соответствии с планом.

Реферат завершается выводами, в которых необходимо показать отношение **автора реферата** к рассматриваемой проблеме и пути её решения.

6. Преподавательский состав, реализующий дисциплину

Беляев Виктор Афанасьевич, канд. техн. наук, доцент кафедры компьютерной безопасности института прикладной математики и компьютерных наук НИ ТГУ.

7. Язык преподавания – русский язык.